METHOD FOR PERFORMING SEGMENTING LOCKING AND MERGING CONTROL OF ENCRYPTED DIGITAL ASSETS BASED ON TIME DIMENSION

RELATED APPLICATIONS

[0001] This application is a "bypass" continuation-in-part of PCT Application Number PCT/CN2018/089805 filed 4 Jun. 2018; the contents of which are hereby incorporated by reference.

FIELD OF TECHNOLOGY

[0002] The present invention relates to the technical field of blockchain, in particular to the technical field of time division of encrypted digital assets, specifically, it refers to a method for performing segmenting locking and merging control of encrypted digital assets based on time dimension.

DESCRIPTION OF RELATED ARTS

[0003] At present, typical digital assets controlled and managed by a key take encrypted digital currency as an example, digital currency has two attributes, one is the name of a currency, and the other is its value, which is usually described in the form of a certain number of digital currencies.

[0004] Here we mark the name of the digital currency as N and its corresponding amount as M, then no matter whether the blockchain uses UTXO (Unspent Transaction Outputs) or the account system of Account, from the perspective of the user, the assets that some user holds at a certain moment could be represented by the following model:

(N, M);

[0005] namely, the user owns M encrypted digital currencies named N.

[0006] Correspondingly, what the existing blockchain realizes is to segment the digital assets held by users in quantity, for example, divide (N, M) at the current moment into (N, m1) and (N, m2) at the next moment, where:

$M=m1+m2$;

[0007] according to this, we can see that such segmentation is an atomic segmentation of digital assets about quantity at a certain point in time, which is suitable for application scenarios of instant transaction settlement.

[0008] However, as we know, in the traditional financial field, the existence of financial activities and businesses about future value rights, for example, accept a bill of exchange, is based on the payer's credit standing and respectability (comprises mortgage and credit), the bank acts as a third-party attestation and guarantee, ensure to unconditional payment of a certain amount to the payee on the specified date, to realize financial behavior that the exchange of value across time. On the basis of accept a bill of exchange, commercial transaction financing further derives acceptance financing business and markets.

[0009] In the field of crypto finance, there are also financial behaviors that realize unconditional payment of a certain value to a specific payer on a specified date for encrypted digital currency. But current digital currencies such as Bitcoin do not have this function.

SUMMARY OF THE INVENTION

[0010] The object of the present invention is to overcome the drawbacks of the prior arts, to provide a method for performing segmenting locking and merging control of encrypted digital assets based on time dimension.

[0011] In order to achieve the above objects, the present invention of method for performing segmenting locking and merging control of encrypted digital assets based on time dimension has the following composition:

[0012] The method for performing segmenting locking of encrypted digital assets based on time dimension, characterized in that, the said method comprises: a first user terminal stores a first encrypted digital asset (N, M) in a first data structure which belongs to the first user terminal, and add attributes for a time period interval (T1, T2) of the first encrypted digital asset (N, M) to a second data structure which belongs to the first user terminal, in order to expand the first encrypted digital asset (N, M) into a second encrypted digital asset (N, M, T1, T2) having attributes for the time period interval (T1, T2); based on the second data structure, the first user terminal's ownership related to the first encrypted digital asset (N, M) in the time period interval (T1, T2) could be separated into the right to use of a second user terminal related to the first encrypted digital asset (N, M) in a time period interval (T1, P), and the first user terminal's ownership related to the first encrypted digital asset (N, M) in a time period interval (P+1, T2), the said T1, P, T2 are any positive integers, and the $T1<P<T2$.

[0013] In the method for performing segmenting locking of encrypted digital assets based on time dimension, the said first data structure is data structure of Account, the second data structure is data structure of UTXO or data structure of Hybrid Model.

[0014] In the method for performing segmenting locking of encrypted digital assets based on time dimension, before the first user terminal's ownership related to the first encrypted digital asset (N, M) in the time period interval (T1, T2) is separated, the second data structure needs to receive a transfer request related to the first encrypted digital asset (N, M) initiated by the first user terminal in a first account model, the transfer request comprises the time point parameter P.

[0015] In the method for performing segmenting locking of encrypted digital assets based on time dimension, the said right to use comprises the transfer and exchange of the first encrypted digital asset (N, M).

[0016] In the method for performing segmenting locking of encrypted digital assets based on time dimension, after the first user terminal's ownership related to the first encrypted digital asset (N, M) in the time period interval (T1, T2) is separated, the first data structure will eliminate the transferred first encrypted digital asset (N, M).

[0017] A method for realizing merging control of encrypted digital assets based on time dimension, based on the above method for segmenting locking, characterized in that, the said method comprises: in the second data structure, based on the first user terminal's ownership related to the first encrypted digital asset in the time period interval P+1 to T2, and according to that after the right to use of the second user related to the first encrypted digital asset in the time period interval Q to P has been obtained, the first user terminal could obtain the ownership related to the first encrypted digital asset in the time period Q to T2, the said Q is any positive integers, and the $T1<Q<P<T2$.